Google Scholar BETA

Blogs Books ...es Video News Maps **more »**

VMM TPM hypervisor Paul England Search

Groups Patents **Scholar even more »**

Advanced Scholar Search
Scholar Preferences
Scholar Help

Scholar Resu... **English** pages for **VMM TPM hypervisor Paul England**. (**0.10** seconds)

Virtual machines for ente...top security
P **England**, J Manferdelli - Information Security Technical Report, 2006 - Elsevier
... Although not shown, a microkernel **hypervisor** has similar **...** and further adding the administration cost of a **VMM**. **...** With **TPM** and other hardware support, there would **...**
Cited by 1 - Related articles - Web Search - All 2 versions

Practical Techniques for Operating System Attestation
P **England** - Trusted Computing Challenges and Applications: First ..., 2008 - books.google.com
... a PCR (or virtual PCR) by the **hypervisor**.[T6] The **...** pair and uses the **TPM** (or virtual **TPM**)" Qwoie" facility **...** and necessary behavior of the OS and **VMM** for brevity. **...**
Web Search

Local secure service partitions for operating system security
TV Kurien, P **England**, RN Pandya, N Ferguson - US Patent App. 11/097,697, 2005 - Google Patents
... 76) Inventors: Thekkthalackal Varugis Kurien, Sammamish, WA (US); **Paul England**, Bellevue, WA **...** integrity has been measured by the **TPM** or a trusted **hypervisor**. **...**
Web Search

Integration of high-assurance features into an application through application factoring
TV Kurien, KD Ray, M Peinado, P **England** - US Patent App. 10/693,749, 2003 - Google Patents
... D. Ray, Seattle, WA (US); Marcus Peinado, Bellevue, WA (US); **Paul England**, Bellevue, WA **...** itself from tampering—eg, a trusted processor module (**TPM**), a memory **...**
Web Search - All 2 versions

Integration of high-assurance features into an application through application factoring
KD Ray, M Peinado, P **England**, TV Kurien - EP Patent 1,526,456, 2005 - freepatentsonline.com
... from tampering - eg, a trusted processor module (**TPM**), a memory **...** 508 are a virtual machine monitor (**VMM**), an exokernel, a microkemel, or a **hypervisor**. **...**
Related articles - Web Search - All 3 versions

Key authors: **P England** - **T Kurien** - **K Ray** - **M Peinado**

VMM TPM hypervisor Paul England Search